ENCLOSURE 1

M220163

White Paper

NEDO-33989, Revision 0
BWRX-300 Safety Strategy White Paper

Non-Proprietary Information

HITACHI

GE Hitachi Nuclear Energy

NEDO-33989
Revision 0
December 2022

Non-Proprietary Information

White Paper

BWRX-300 Safety Strategy

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

The design, engineering, and other information contained in this document is furnished for the purpose of facilitating collaborative review by the Canadian Nuclear Safety Commission (CNSC) and Nuclear Regulatory Commission (NRC) regarding the acceptability of the licensing approach and plan for additional submittals regarding the BWRX-300 Small Modular Reactor design and licensing basis information contained herein. The only undertakings of GE Hitachi Nuclear Energy Americas LLC (GEH) with respect to information in this document are contained in the contracts between GEH and its customers or participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone for any purpose other than that for which it is intended is not authorized; and with respect to any unauthorized use, GEH makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

REVISION SUMMARY

Revision Number	Description of Change
0	Initial Issue

Acronyms and Abbreviations

Term	Definition
ABWR	Advanced Boiling Water Reactor
ACM	Availability Controls Manual
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrence
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
BL-AOO	Baseline Anticipated Operational Occurrence
BL-DBA	Baseline Design Basis Accident
BL-DSA	Baseline Deterministic Safety Analysis
B&PV	Boiler and Pressure Vessel
BWR	Boiling Water Reactor
CCF	Common Cause Failure
CDF	Core Damage Frequency
CIV	Containment Isolation Valve
CN-DBA	Conservative Design Basis Accident
CN-DSA	Conservative Deterministic Safety Analysis
CNSC	Canadian Nuclear Safety Commission
CPA	Construction Permit Application
CSA	Canadian Standards Association
DBA	Design Basis Accident
DEC	Design Extension Condition
DL	Defense Line
D-in-D	Defense-in-Depth

Term	Definition
DPS	Diverse Protection System
DSA	Deterministic Safety Analysis
EHE	External Hazard Evaluation
EOP	Emergency Operating Procedure
ESBWR	Economic Simplified Boiling Water Reactor
EX-DBA	Extended Design Basis Accident
EX-DEC	Extended Design Extension Condition
EX-DSA	Extended Deterministic Safety Analysis
FFHE	Functional Failure Hazard Evaluation
FMEA	Failure Modes and Effects Analysis
FSF	Fundamental Safety Function
GDC	General Design Criteria
GEH	GE Hitachi Nuclear Energy Americas LLC
HGNE	Hitachi-GE Nuclear Energy Ltd
HOHE	Human Operation Hazard Evaluation
IAEA	International Atomic Energy Agency
IE	Initiating Event
IEEE	Institute of Electrical and Electronics Engineers
IHE	Internal Hazard Evaluation
LRF	Large Release Frequency
LTR	Licensing Topical Report
PAM	Post-Accident Monitoring
PIE	Postulated Initiating Event
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
RCPB	Reactor Coolant Pressure Boundary

Term	Definition
RG	Regulatory Guide
RIPB	Risk-Informed Performance-Based
RPV	Reactor Pressure Vessel
SA	Severe Accident
SAFDLs	Specified Acceptable Fuel Design Limits
SAA	Severe Accident Analysis
SBO	Station Blackout
SMR	Small Modular Reactor
SSC	Structure, System, and Component
SRP	Standard Review Plan
TS	Technical Specifications
USNRC	U.S. Nuclear Regulatory Commission

1.0 INTRODUCTION

BWRX-300 is an approximately 300 MWe, water cooled, natural circulation Small Modular Reactor (SMR) utilizing simple passive safety systems driven by natural phenomena. It is developed by GEH in the U.S. and Hitachi-GE Nuclear Energy Ltd (HGNE) in Japan. It is the tenth generation of the Boiling Water Reactor (BWR). BWRX-300 is an evolution of the US NRC-certified design for the 1,520 MWe Economic Simplified Boiling Water Reactor (ESBWR).

1.1 Purpose

The purpose of this white paper is to request feedback from the U.S. Nuclear Regulatory Commission (USNRC) and Canadian Nuclear Safety Commission (CNSC) regarding the proposed use of the Safety Strategy for the GE Hitachi Nuclear Energy Americas LLC (GEH) BWRX-300 Small Modular Reactor (SMR). The BWRX-300 Safety Strategy incorporates selected guidance from the International Atomic Energy Agency (IAEA) Safety Standards Specific Safety Requirements No. SSR-2/1, Revision 1, "Safety of Nuclear Power Plants: Design." However, GEH is not requesting specific regulatory endorsement of IAEA SSR-2/1 by either the USNRC or CNSC, only feedback concerning the Safety Strategy as presented in this white paper.

The BWRX-300 Safety Strategy forms the basis for the BWRX-300 Safety Analysis Reports (SARs) (i.e., the Safety Analysis) developed to support licensing applications for construction and operation of the BWRX-300 in the U.S. and Canada. The Safety Strategy includes identification of postulated initiating events (PIEs) and development of Fault Sequences based on standard plant design internal and site-specific external Hazard Evaluations. The Safety Strategy uses a defense-in-depth (D-in-D) safety concept providing a layered and iterative approach to plant safety while meeting USNRC and CNSC regulatory requirements and guidance.

The BWRX-300 Safety Strategy framework considers both the safety-importance and risk-significance of each structure, system, and component (SSC) to determine the design requirements and appropriate safety and quality classification for each SSC. The BWRX-300 Safety Strategy includes the use of a risk-informed performance-based (RIPB) approach consistent with the scope, criteria, and process described in USNRC NUREG-0800, "Standard Review Plan of the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Standard Review Plan (SRP) 19.3, "Regulatory Treatment of Nonsafety Systems for Passive Advanced Light Water Reactors" (ADAMS Accession No. ML14035A149), CNSC REGDOC-2.4.2, "Probabilistic Safety Assessment (PSA) Nuclear Power Plants," and Canadian Standards Association (CSA) N290.17-17 "Probabilistic Safety Assessment for Nuclear Power Plants."

1.2 Scope

The scope of this document includes the following applicability to USNRC and CNSC regulatory requirements and guidance:

- BWRX-300 Safety Strategy concept, including a description of the Fundamental Safety Functions (FSFs), D-in-D concept and process for plant and system design requirements
- Defense Line (DL) definition and application, including process and guidance for classification of SSCs

- Description of the Safety Analysis objectives, scope, and approach that aligns with the BWRX-300 Safety Strategy
- Description of the identification, categorization and grouping of Postulated Initiating Events (PIEs) and accident scenarios, including Fault Sequences
- Description of the Hazard Evaluation process and the Deterministic Safety Analysis (DSA) and Probabilistic Safety Assessment (PSA) processes

2.0 BWRX-300 Safety Strategy

The overall safety philosophy for the design of the BWRX-300 is referred to as the Safety Strategy. The objective of the Safety Strategy is to establish a design with a high level of safety using D-in-D concepts. This is accomplished through incorporation of design requirements using selected guidance from IAEA Specific Safety Requirements SSR-2/1. Design requirements in CNSC REGDOC-2.5.2, "Design of Reactor Facilities: Nuclear Power Plants," and USNRC 10 CFR 50, Appendix A, "General Design Criteria (GDC) for Nuclear Power Plants," are consistent with the principles set forth in the Safety Strategy described in this report.

2.1 Applying the Safety Principles and Concepts

Fundamental Safety Principles as described in IAEA SSR 2/1 establish the safety objective and safety principles that provide the basis for requirements and measures for the protection of people and the environment against radiation risks and the safety of facilities and activities that give rise to radiation risks. The safety principles include the following measures used in the design of the BWRX-300:

1. Controlling radiation exposures to workers and the public and radioactive releases to the environment in all plant states
2. Restricting the likelihood of events in all plant states that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source, spent nuclear fuel, radioactive waste or any other source of radiation at a nuclear power plant mitigating the consequences of such events if they were to occur. The Fundamental Safety Principles apply to all stages of the nuclear power plant lifetime.

2.1.1 Radiation Protection in Design

In order to satisfy the Fundamental Safety Principles, the BWRX-300 design includes measures for all plant states and for any activities ensuring that doses from radiation exposure within the BWRX-300 plant or exposure due to any planned radioactive release from the BWRX-300 are kept below the allowed dose limits and kept as low as reasonably achievable (ALARA). The design includes measures for mitigating the radiological consequences of any accidents in the unlikely event they were to occur.

2.1.2 Safety in Design

The BWRX-300 design includes measures consistent with acceptance criteria and safety objectives established by the CNSC and USNRC in their respective regulatory requirements and guidance:

1. Preventing accidents with harmful consequences resulting from a loss of control over the reactor core or over other sources of radiation, and mitigating the consequences of any accidents that do occur
2. Ensuring all accidents are taken into account in the design of the installation, and any resulting radiological consequences are below the relevant limits and kept ALARA
3. Ensuring the likelihood of occurrence of an accident with serious radiological consequences is extremely low and that the radiological consequences of such an accident are mitigated to the fullest extent practicable

2.1.3 The D-in-D Concept

The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is applying the D-in-D concept . This concept is applied to all plant states (full power, low power or shutdown states and all fault sequences) and the associated plant response is used in establishing the plant design that takes into account internal, external, and human hazards. This ensures that plant transients are detected, controlled, monitored, and mitigated with independent layers of defense and compensated for or corrected by appropriate measures. Applying the D-in-D concept throughout design and operation provides protection against anticipated operational occurrences (AOOs) and design basis accidents (DBAs), including those resulting from equipment failure or human induced events within the plant, and the consequences of external events.

2.1.4 Maintaining the Integrity of the Design Throughout the Lifetime of the Plant

The design, construction and commissioning of a nuclear power plant might be shared between organizations, including the architect–engineer, the vendor of the reactor and its supporting systems, the suppliers of major components, the designers of electrical systems, and the suppliers of other systems that are important to the safety of the plant. The prime responsibility for safety rests with the person or organization responsible for facilities and activities that give rise to radiation risks (i.e., the operating organization).

In practice, the design of a nuclear power plant is complete only when the full plant specification (including site details) is produced for procurement and licensing. For the BWRX-300, GEH is the formally designated responsible designer (Design Authority) that has overall responsibility for the design process and is responsible for approving design changes and ensuring that the requisite knowledge is maintained. GEH also has design partners (other responsible designers) who are responsible for assigned portions of the plant design. Prior to an application for construction of a BWRX-300 unit, the responsibility for the design rests with GEH and designated responsible designers. Once a construction application has been made, the prime responsibility for safety lies with the applicant, although detailed design knowledge rests with the Design Authority and responsible designers. This balance changes as the plant is put into operation, since much of this detailed knowledge, such as the knowledge embodied in the SAR, design manuals, and other design documentation are transferred to the operating organization.

2.2 Management of Safety in Design

Responsibilities management of the BWRX-300 plant design include the following requirements from the BWRX-300 Safety Strategy.

2.2.1 Responsibilities in Management of Safety in Plant Design

An applicant for construction and operation of the BWRX-300 is responsible for ensuring that the design submitted to the regulatory authority meets all applicable safety requirements.

2.2.2 Management of Systems for Plant Design

The GEH Design Authority establishes and implements the BWRX-300 design management system ensuring that all safety requirements established for the design are considered and implemented in all phases of the design process and that they are met in the final design.

The management system includes provisions for ensuring the design quality of each SSC, as well as of the overall design of the BWRX-300 at all times. This includes the means for identifying and correcting design deficiencies, checking the adequacy of the design, and controlling design changes.

2.2.3 Safety of the Plant Design Throughout the Lifetime of the Plant

The operating organization is responsible for establishing a formal system that ensures the continuing safety of the plant design throughout the nuclear power plant lifetime.

2.3 Principle Technical Requirements

Principle technical requirements considered in the design of the BWRX-300 include the following requirements.

2.3.1 Fundamental Safety Functions

The following Fundamental Safety Functions (FSFs) meet the requirements of USNRC 10 CFR 50, Appendix A GDCs, CNSC REGDOC-2.5.2, "Design of Reactor Facilities: Nuclear Power Plants," and CNSC REGDOC-2.4.1 "Deterministic Safety Assessment (DSA) for Nuclear Power Plants":

- Controlling reactivity
- Removing heat from the fuel (in the reactor, during fuel storage and handling, and long-term heat removal)
- Confining radioactive materials, shielding against radiation and controlling planned radioactive releases, and limiting accidental releases

The FSFs prevent or mitigate radioactive releases by ensuring the physical barriers to releases remain effective. The physical barriers include the fuel matrix, fuel cladding, Reactor Coolant Pressure Boundary (RCPB), and Containment that meet the requirements of USNRC 10 CFR 50.2 definition of safety-related and CNSC REGDOC-2.5.2. In addition to the protection of barriers, a means of monitoring the status of key plant parameters is provided for ensuring that the FSFs are fulfilled. From this perspective, the monitoring function is treated as inherent to the design of the FSF. Other considerations for the monitoring function are as follows:

1. If a manual operator action plays a role in performing an FSF, the monitoring function of the equipment used to display key plant parameters that are necessary for the operator to perform the manual action successfully are also considered part of the FSF.
2. Certain monitoring functions allow the operator to confirm ongoing effectiveness of the FSFs during all plant states, to implement post-accident procedures, and to make decisions in supporting emergency planning.

3. Post-Accident Monitoring (PAM) is important for operator decision making such as taking manual actions and implementing functions. Therefore, the designation, treatment and display of certain plant parameters or measurements as PAM variables is a supporting design feature.
4. A minimum set of monitoring functions and display of parameters that do not support the operator actions are provided to support accident assessment.

Preservation of the FSFs is intrinsic to the BWRX-300 Safety Strategy. A systematic approach is taken to identify the functions and SSCs necessary to fulfill the FSFs following a PIE or a Fault Sequence. The BWRX-300 Safety Strategy Flow Chart shown on Figure 2-1 illustrates the iterative methodology used in developing the DLs that ensures the FSFs are maintained, thus complying with applicable regulatory requirements. Defense Line definitions and application within the BWRX-300 Safety Strategy are presented in Section 3.

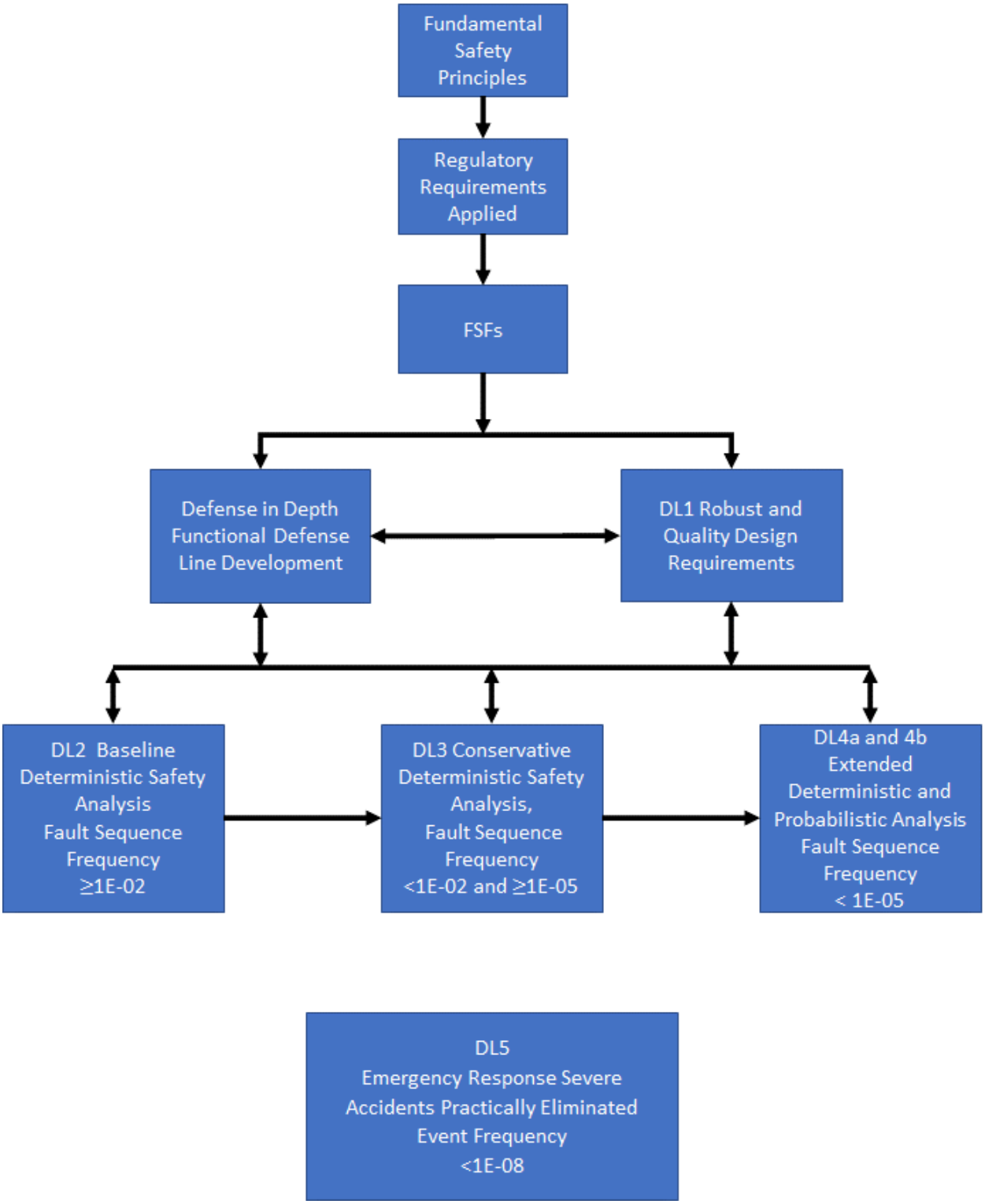

Figure 2-1: BWRX-300 Safety Strategy Flow Chart

2.3.2 Radiation Protection in Design

The BWRX-300 design ensures that plant states that could lead to high radiation doses or to early or large radioactive release have been "practically eliminated," and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence. Acceptable limits for radiation protection associated with the relevant plant states categories are established consistent with the applicable regulatory requirements.

2.3.3 BWRX-300 Safety Design

The BWRX-300 Safety Strategy includes appropriate characteristic and design parameter requirements for equipment and structures important to safety to ensure:

- safety functions can be performed with the necessary reliability
- the plant can be operated safely within the operational limits and conditions for the full duration of its design life
- the plant can be safely decommissioned
- environmental impacts are minimized

2.3.4 Application of D-in-D Concept

The D-in-D implementation in the BWRX-300 design forms the basis for the BWRX-300 Safety Strategy ensuring an adequate level of safety is achieved.

The D-in-D concept involves the provision of multiple layers of defense or DLs against some undesirable outcome. In the case of a nuclear power plant, the undesirable outcome is the exposure of workers, the public or the environment to radioactivity exceeding levels determined to be safe.

There are two types of defensive layering considered:

1. Physical barriers prevent the release of radioactivity, including the fuel matrix, fuel cladding, RCPB, and containment. The integrity of one or more physical barriers is maintained to prevent unacceptable releases.
2. A combination of active, passive, and inherent safety features used in the design minimizes challenges to the physical barriers, maintains the integrity of the barriers and, in case a barrier is breached, ensures the integrity of the remaining barriers.

While the physical barriers themselves represent multiple layers of defense against radioactive releases, in the BWRX-300 D-in-D application, the physical barriers are not themselves referred to as DLs. This term is reserved for the layers of defense comprising features, functions and practices that protect the integrity of the barriers. The fundamental purpose of the DLs is ensuring the integrity of the physical barriers by applying multiple levels of protection (further defined in Section 3.0).

The BWRX-300 D-in-D concept uses the FSFs described above to define the relationship between the DLs and the physical barriers. For each Fault Sequence, if the FSFs are performed successfully, then the corresponding physical barriers remain effective.

2.3.5 Developing the Plant Design Basis

The general plant design requirements (i.e., design rules) for SSCs performing FSFs are established based on considering the following:

- Design basis requirements:
  - Applicable plant operating states (Operational Modes 1-6) considered in the Safety Analysis applicable to SSCs performing FSFs
  - Consideration of Internal and External Hazard (including Site-Specific External Hazards) Evaluations meeting the following requirements:
    - USNRC 10 CFR 50, Appendix A, GDC 2 “Design Bases for Protection Against Natural Phenomena”
    - USNRC 10 CFR 50, Appendix A, GDC 3 “Fire Protection”
    - USNRC 10 CFR 50, Appendix A, GDC 4 “Environmental and Dynamic Effects Design Bases”
    - CNSC REGDOC-2.5.2, Sections 7.4.1 “Internal hazards” and “External hazards”
  - Consideration of PIEs and development of Fault Sequences, including determination of the DL functions (DL2, DL3, DL4a, and DL4b) credited for mitigating the consequences of the Fault Sequences to meet applicable Safety Analysis acceptance criteria, including consideration of:
    - Fault Sequences for Design Basis Events, including AOOs and DBAs
    - Fault Sequences for Design Extension Conditions (DECs), both without and with core damage
    - Licensing Basis Events included in specific USNRC regulatory requirements and guidance, such as Anticipated Transient Without Scram (ATWS) (10 CFR 50.62) and Station Blackout (SBO) (10 CFR 50.63), and CNSC REGDOC-2.5.2, Section 8.4 “Means of shutdown” and Section 8.9.3 “Alternate AC power supply”
  - Consideration of SSC functions that provide defense barriers against Fault Sequences that challenge safety, including design rules for diversity, separation, redundancy, independence, and reliability meeting the following requirements:
    - USNRC 10 CFR 50, Appendix A, GDC 21 “Protection System Reliability and Testability”
    - USNRC 10 CFR 50, Appendix A, GDC 22 “Protection System Independence”
    - CNSC REGDOC-2.5.2, Section 7.6.1.1 “Separation”
    - CNSC REGDOC-2.5.2, Section 7.6.1.2 “Diversity”
    - CNSC REGDOC-2.5.2, Section 7.6.1.3 “Independence”
  - Consideration of SSC Safety Classes (SC) as defined in Section 3.7, including SC1, SC2, SC3, and SCN, and determination of applicable SSC classifications, meeting the following requirements:

  - USNRC 10 CFR 50.2 “Definitions” “Safety-related”, USNRC 10 CFR 50, Appendix B “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”
  - USNRC RG 1.26 “Quality Group Classifications and Standards for Water-, Steam-, and Radioactive-Waste-Containing Components of Nuclear Power Plants”
  - USNRC 10 CFR 50, Appendix S “Earthquake Engineering Criteria for Nuclear Power Plants”
  - USNRC RG 1.29 “Seismic Design Classification for Nuclear Power Plants”
  - CNSC REGDOC-2.5.2, Section 7.1 “Safety classification of structures, systems and components”
  - REGDOC-2.5.2, Section 7.13 “Seismic qualification and design”
  - CSA N289.1 “General Requirements for Seismic Design and Qualification of Nuclear Power Plants,” Clause 5.2.5.2
- Consideration of Common Cause Failures (CCFs) included in the Fault Sequences both as PIEs and in conjunction with other PIEs meeting the following requirements:
  - USNRC 10 CFR 50, Appendix A, GDC 21, “Protection System Reliability and Testability”
  - USNRC 10 CFR 50, Appendix A, GDC 22, “Protection System Independence”
  - CNSC REGDOC-2.5.2, Section 7.6.1 “Common Cause Failures”
- Single failure criterion for SC1 equipment
  - USNRC 10 CFR 50, Appendix A
  - CNSC REGDOC-2.5.2, Section 7.6.2 “Single failure criterion”
  - CNSC REGDOC-2.4.1, Section 4.4.4 “Assumptions for deterministic safety analysis”
- Operational limits and conditions (OLCs) for safe operation
  - USRNC technical specifications (TS) 10 CFR 50.36
  - CNSC REGDOC-2.5.2, Section 4.3.3 “Operational, limits and conditions”
- Calibration, testing, maintenance repair, inspection and monitoring of items important to safety
  - USNRC 10 CFR 50, Appendix A “General Design Criteria for Nuclear Power Plants”
  - USNRC 10 CFR 50, Appendix B “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”
  - USNRC 10 CFR 50.65 “Requirements for monitoring the effectiveness of maintenance at nuclear power plants”
  - CNSC REGDOC-2.5.2, Section 5.3 “Design control measures”

- Consideration of human factors in the design of SSCs meeting the following requirements:
  - USNRC 10 CFR 50.34(f)) “Contents of applications: technical information”
  - USNRC NUREG-0711, “Human Factors Engineering Program Review Model”
  - USNRC NUREG-0737 “Clarification of Three Mile Island Action Plan Requirements”
  - “”REGDOC-2.5.2 Section 7.21 “Human factors”
  - CNSC REGDOC-2.4.2 “Probabilistic Safety Assessment for Nuclear Power Plants”
  - CSA N290.17-17 “Probabilistic Safety Assessment for Nuclear Power Plants”

3.0 Defense Line Definitions and Application

Five DLs (or levels), DL1 through DL5, are adopted. Figure 3-1 illustrates the DLs and corresponding plant states.

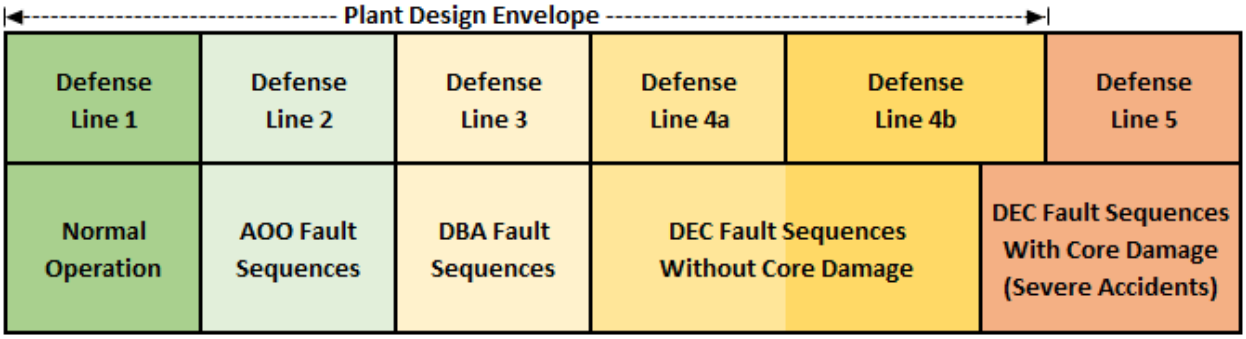

Figure 3-1: D-in-D – Plant States and DLs

DL1 minimizes the potential for PIEs to occur and the potential for failures in DL1, DL2, and DL4 by assuring high quality and conservatism in the design, construction, and operation. DL2, DL3, and DL4 comprise plant functions that act to prevent PIEs from leading to loss of FSFs or control events that can potentially lead to significant radiological release or exposure. DL5 involves emergency preparedness to protect the plant staff, emergency workers, and the public in case a substantial radioactive release occurs.

The DL1 measures and DL2, DL3, and DL4 functions are incorporated to ensure:

- The normal operation of the plant is monitored, detected, and controlled so that PIEs leading to AOOs are detected and conditions controlled before evolving into DBAs
- The consequences are limited if a DBA develops
- Multiple DLs are capable of independently performing the FSFs. While this means that more than one DL is capable of independently performing the FSFs for D-in-D, DL independence from all other DLs is based on how specific DLs are credited for specific PIEs

Reliability target goals are established for each DL function that conforms with the following USNRC Commission SECY papers that are invoked and form the basis of USNRC SRP 19.3. The reliability target goals also comply with CNSC REGDOC-2.5.2, Section 2.2.2 “Safety goals,” Section 3.5 “Operational experience and safety research,” Section 5.5 “Design rules and limits,” and Section 5.6 “Design for reliability”:

- USNRC SECY-93-087 “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor ALWR Designs,” dated April 2, 1993 (ADAMS Accession No. ML003760768), and associated SRM, July 21, 1993 (ADAMS Accession No. ML003708056)
- USNRC SECY-94-084, “Policy and Technical Issues Associated with the Regulatory Treatment of Nonsafety Systems in Passive Plant Designs,” dated March 28, 1994, and associated SRM, June 30, 1994 (ADAMS Accession No. ML003708068)

- USNRC SECY-95-132, "Policy and Technical Issues Associated with the Regulatory Treatment of Nonsafety Systems (RTNSS) in Passive Plant Designs," dated May 22, 1995, and associated SRM, June 28, 1995
- USNRC SECY-11-0024 "Use of Risk Insights to Enhance the Safety Focus of Small Modular Reactor Reviews," dated February 18, 2011, and associated SRM, May 11, 2011

In USNRC SECY-94-084 the Commission stated: " … the Commission (with all Commissioners agreeing) has approved the staff's recommendation on Regulatory Treatment of Non-Safety Systems (RTNSS). The Chairman believes that the licensees should use the complete plant PRA as opposed to the "focused PRA" to provide an integrated assessment of the relative importance of various systems and components. The focused PRA model does not include some non-safety systems whose performance would affect the calculated risk contribution. Other methods, perhaps utilizing risk importance measures, could be identified which still incorporate the information of the complete PRA. The Chairman requested that the staff evaluate this approach."

The "other methods" used by the ESBWR was to augment the focused Probabilistic Risk Assessment (PRA) results by identifying nonsafety-related equipment that reduced the core damage frequency (CDF) to below the safety goals of the Commission.

The USNRC Staff conclusions in NUREG-1966, "Final Safety Evaluation Report Related to the Certification of the Economic Simplified Boiling-Water Reactor Standard Design," included the following:

> "The applicant determined that 10 CFR 50.36(c)(2)(ii) does not require establishing GTS [Generic Technical Specification] LCOs [Limiting Conditions for Operation] for most active nonsafety systems. However, following the guidance in SECY-94-084, "Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems (RTNSS) in Passive Plant Designs," the applicant proposed establishing an ESBWR availability controls manual (ACM), which is described in DCD Tier 2, Revision 9, Chapter 19A. The applicant's evaluation of nonsafety-related systems against the regulatory treatment of nonsafety systems (RTNSS) significance criteria identified those nonsafety-related SSCs which require high regulatory oversight in the form of GTS LCOs; those nonsafety-related SSCs which require low regulatory oversight in the form of short-term availability controls, and which are included in the ACM; and those nonsafety-related SSCs which require only the oversight imposed by 10 CFR 50.65 (referred to as the Maintenance Rule). To address the long-term safety issue in Criterion 2 of Section 22.2 of this report, the design certification applicant will use PRA insights, sensitivity studies, and deterministic methods to establish the ability of the design to maintain core cooling and containment integrity beyond 72 hours.
>
> Nonsafety-related SSCs that are required to meet deterministic regulatory requirements (Criterion 1), resolve the long-term safety and seismic issues (Criterion 2), and prevent significant adverse systems interactions (Criterion 5) are subject to regulatory oversight. The staff expects regulatory oversight for all nonsafety-related SSCs needed to meet USNRC requirements, safety goal guidelines, and containment performance goals, as identified in the focused ESBWR PRA model. Using the focused PRA to determine the nonsafety-related SSCs important to risk involves the following three steps:
>
> 1. Determine those nonsafety-related SSCs needed to maintain the initiating event frequencies at the comprehensive baseline ESBWR PRA levels.

2. Add the necessary success paths (i.e., a Fault Sequence in the PRA event tree that results in no core damage) with nonsafety-related systems and functions to the focused PRA to meet safety goal guidelines, containment performance goal objectives, and USNRC regulations. Choose the systems by considering the factors for optimizing the design effects and benefits of these SSCs."

As part of the BWRX-300 Safety Strategy including the PSA, PRA importance (sensitivity) studies are performed for the BWRX-300 to evaluate whether SC1 system(s) alone are adequate to meet:

- USNRC safety goals of CDF less than 1.0 E-4 per reactor-year and large release frequency (LRF) less than 1.0 E-6 per reactor-year
- CNSC safety goals of CDF less than 1.0 E-05 per reactor-year and LRF sum of frequencies of all Fault Sequences that can lead to a release to the environment of more than 10^{14} becquerels of cesium-137 less than 1.0 E-06 per reactor-year

The PRA studies, which encompass at-power and shutdown modes for internal and external events, retain the same initiating event frequencies as the baseline PRA models, and set the logic status of non-SC1 systems to fail, while SC1 systems remain unchanged in the models. The need for non-SC1 systems to meet the CDF and LRF goals are determined and evaluated within the PRA models. Additional non-SC1 systems are included only if they are required to meet the CDF or LRF goals.

USNRC SECY-11-0024 states the following:

> "The framework incorporates a more risk-informed approach to the staff's review by considering both the safety-importance and risk-significance of each SSC to help determine the appropriate level of review for each SSC. In this regard, the framework is similar to USNRC 10 CFR 50.69, "Risk-informed categorization and treatment of structures, systems, and components for nuclear power reactors." Risk-significance may be determined using a process similar to that used in identifying those SSCs included in the reliability assurance program (DC/COL-ISG-018, "Interim Staff Guidance on NUREG-0800 Standard Review Plan Section 17.4, "Reliability Assurance Program") and the results of that determination are used to guide the remainder of the review process."

Reliability target goals expressed in failures per demand are established for the DL functions:

- DL3 functions – <1E-04 probability of failure per demand
- DL4a functions – <1E-03 probability of failure per demand
- DL2 and DL4b functions – <1E-02 probability of failure per demand

Table 3-1 provides a high-level description of the objective, design means, and operational means for supporting the DLs.

Table 3-1: Identification of Defense Lines

DL	Objective	Design Means	Operational Means
DL1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Operational rules and normal operating procedures
DL2	Control of abnormal operation and detection of failures	System functions for limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures
DL3	Control of design basis accidents	System functions for engineered safety features	Emergency operating procedures
DL4a	Control of design extension conditions to prevent core damage	System functions for safety features for design extension conditions without core damage	Emergency operating procedures
DL4b	Control of design extension conditions to prevent or mitigate the consequences of severe accidents	System functions for safety features for design extension conditions that may result in core damage	Emergency operating procedures/Severe Accident management guidelines (SAMG)
DL5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans

The DL functions used in detecting and controlling AOOs and mitigating DBAs and DECsand failures assessed in each event category, are evaluated in the DSA to identify those design feature(s) (i.e., design functions) that prevent the event from escalating into the next event category.

Design rules are used in establishing the performance-based design requirements including assignment of DL functions and SSC classification for those SSCs used in detecting, monitoring, and mitigating events, including consideration of:

- Primary and integral support DL functions
- Single failure criterion
- Independence from other DL functions to the extent practicable (Defined in Section 3.6)
- Physical separation within each DL function
- Physical separation from other DL functions
- PSA treatment of DL functions including modeling requirements
- Manual initiation capabilities
- Functional qualification requirements

- Environmental qualification requirements
- Seismic Category determination
- Reliability assurance program applicability
- TS or OLC development for LCOs established for DL3 and selected DL2 functions
- ACM development, as required by TS or OLC, for DL4a, DL4b, and selected DL2 functions
- Quality requirements
- Protection requirements against design basis internal and external events
- Pre-service and In-service inspection and testing requirements
- Uninterruptible power requirements
- Backup power requirements and classification
- Design Provisions to support functions in various DLs

3.1 Defense Line 1

The purpose of the first line of defense is to prevent deviations from normal operation and the failure of important SSCs. This is achieved by implementing design process and quality measures that minimize the potential for failures and initiating events occurring in the first place and minimizing the potential for failures to occur in subsequent lines of defense. These quality measures cover the lifecycle of the plant, including design, construction, commissioning, operation, use of operational experience (OPEX), periodic safety reviews, maintenance, inspection, and testing.

DL1 includes design process and quality measures where the plant safety design complies with, but are not limited to, the following USNRC and CNSC regulatory requirements:

- USNRC 10 CFR 50.34, “Contents of applications; technical information”
- USNRC 10 CFR 50.36, “Technical specifications”
- USNRC 10 CFR 50.44, “Combustible gas control for nuclear power plants”
- USNRC 10 CFR 50.49, “Environmental qualification of electrical equipment important to safety for nuclear power plants”
- USNRC 10 CFR 50.65, “Requirements for monitoring the effectiveness of maintenance at nuclear power plants”
- USNRC 10 CFR 50.69, “Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors”
- USNRC 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants”
- USNRC 10 CFR 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”
- USNRC 10 CFR 50, Appendix S, “Earthquake Engineering Criteria for Nuclear Power Plants”

- CNSC REGDOC-1.1.2, "Licence Application Guide: Licence to Construct a Reactor Facility"
- CNSC REGDOC-1.1.3, "Licence Application Guide: Licence to Operate a Nuclear Power Plant"
- CNSC REGDOC-2.5.2, "Design of Reactor Facilities"
- CNSC REGDOC-2.4.1, "Deterministic Safety Analysis"

Complying with USNRC and CNSC regulations is achieved through the design processes and quality measures used in establishing a robust and conservative plant safety design with safety margin.

Other DL1 design process and quality measures include:

- Defining normal and abnormal operating conditions
- Providing design and safety margins
- Applying appropriate industry standards (e.g., ASME, IEEE, IEC, ANSI, ANI, and CSA)
- Providing comprehensive testing programs
- Establishing conservative and robust design processes and verification
- Reviewing OPEX for changes in the design
- Reviewing extensive BWR fleet data that is applied to the design
- Providing provisions for operators to timely respond to events with appropriate human-machine interfaces, including operator aids reducing their burden
- Evaluating the DSA that includes appropriate conservatism, supplemented by the PSA to produce risk insights to the system design evolution
- Classifying and qualifying SSCs according to their safety significance

DL1 design process and quality measures may support the basis for assumptions made in the Safety Analysis. For example, the use of a high-quality design process and stringent equipment qualification for the most important components support the assumption that only a single failure is considered in the Conservative DSA (CN-DSA).

3.2 Defense Line 2

The purpose of the second line of defense is to provide SSC functions to monitor, detect, control, and mitigate deviations from normal operational states reducing the challenge from AOOs or escalation to accident conditions. The AOO frequency of greater than 1E-02 per reactor-year for requiring DL2 functions meets the definition of AOOs in USNRC 10 CFR 50, Appendix A where AOOs are defined as: "those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of power to all recirculation pumps, tripping of the turbine generator set, isolation of main condenser and loss of all offsite power," and CNSC REGDOC-2.5.2, Section 7.3.2 "Anticipated operational occurrences." Functions that normally operate to maintain key reactor parameters (e.g., pressure, reactor level, and reactivity) within normal ranges are part of DL2 functions.

PIEs in the AOO frequency range of greater than 1E-02 per reactor-year generally include:

- Single failure of non-SC1 digital equipment
- Single failure of non-SC1 digital active equipment
- Single operator error
- Single failure of SC1 digital equipment
- Single failure of SC1 non-digital active equipment
- Some internal and external hazards PIEs

While USNRC NUREG-0800, SRP 15.0 Introduction - Transient and Accident Analyses, Section Areas of Review, Item 6 Event Evaluation, B. Sequence of Events and Systems Operation states that: "the reviewer verifies that the applicant has specified only safety-related systems or components for use in mitigating AOO and postulated accident conditions, and has included single active failures in those systems and components," there is no regulatory basis for asserting that AOOs must be mitigated by safety-related components. The SRP also states that: "the reviewer may consider the licensee's technical justifications for the operation of nonsafety-related systems or components."

BWRX-300 meets this requirement in that all PIEs in the AOO frequency range can be mitigated by DL3 functions if the AOO progresses to a DBA, and DL3 functions are performed by SC1 SSCs which are equivalent to "safety-related SSCs." Because DL2 functions would have to fail for DL3 functions to be required to mitigate the consequences of each AOO, the frequency of the Fault Sequences involving mitigation of AOO PIEs by DL3 functions is in the DBA frequency range, and DBA acceptance criteria are used.

Appropriate design rules are applied to SSCs that are assigned DL2 functions, which are SC3 SSCs (or "nonsafety-related" as defined in the SRP), including the target reliability values discussed above, to provide assurance that a challenge of DL3 functions from an AOO PIE would only occur at a DBA frequency.

The definition of USNRC 10 CFR 50.2 Safety-related structures, systems and components states: "those structures, systems and components that are relied upon to remain functional during and following design basis events to assure:

1. The integrity of the reactor coolant pressure boundary,
2. The capability to shut down the reactor and maintain it in a safe shutdown condition, or
3. The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposure comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable."

Like the predecessor plant ESBWR that is the genesis of the BWRX-300, the BWRX-300 design AOO Fault Sequences do not challenge the integrity of the RCPB ensuring the reactor safely shuts down and is maintained in a safe shutdown condition. There are no DBAs (fault sequencies with frequency events between 1E-02 and 1E-05 per reactor-year) resulting in exposures reaching the limits of either 10 CFR 50.34(a)(1) or 10 CFR 100.11. AOO Fault Sequences do not challenge the integrity of the RCPB and do not lead or escalate to DBA Fault Sequences.

The SRP lists AOO events such as loss of normal feedwater, loss of condenser cooling, single operator error, single failure of control component, and loss of offsite power, all of which are expected SSC failures or PIEs that could occur as part of normal operations. These types of events occur as a result of expected and anticipated equipment failures or errors and are analyzed accordingly. These events are not DBA conditions (frequency events between 1E-02 and 1E-05 per reactor-year) and do not challenge the plant.

The BWRX-300 DL2 functions are performed by SC3 SSCs (nonsafety-related) using specified design rules that include function reliability targets. DL2 functions are backed up by DL3 functions performed by SC1 SSCs (safety-related). This D-in-D approach provides a higher degree of safety than relying solely on DL3 functions. The Safety Analysis for AOO Fault Sequences demonstrate the reliability of the DL2 functions to monitor, detect, and control AOOs, and prevent escalation to a DBA Fault Sequence, conforming with the USNRC SECYs implemented in SRP 19.3 guidance and complying with the requirements of CNSC REGDOC-2.4.2.

Furthermore, the BWRX-300 acceptance criteria established for the AOO Fault Sequences are the specified acceptable fuel design limits (SAFDLs) that are required to be met in the following USNRC 10 CFR 50, Appendix A GDCs and CNSC REGDOC-2.4.1, Section 4.3.4 “Acceptance criteria for anticipated operational occurrences and design-basis accidents:”

- USNRC 10 CFR 50, Appendix A, GDC-10, “Reactor design”
- USNRC 10 CFR 50, Appendix A, GDC-12, “Suppression of reactor power oscillations”
- USNRC 10 CFR 50, Appendix A, GDC-17, “Electric power systems”
- USNRC 10 CFR 50, Appendix A, GDC-20, “Protection system functions”
- USNRC 10 CFR 50, Appendix A, GDC-25, “Protection system requirements for reactivity control malfunctions”
- USNRC 10 CFR 50, Appendix A, GDC-26, “Reactivity control system redundancy and capability”
- USNRC 10 CFR 50, Appendix A, GDC-33, “Reactor coolant makeup”
- USNRC 10 CFR 50, Appendix A, GDC-34, “Residual heat removal”

The use of multiple DLs to control or detect the same PIE using layered DLs cannot reasonably be implemented without a graded acceptance criteria approach as well. DL2 functions backed up by DL3 functions provide a higher degree of safety and justifies applying a graded acceptance criteria to DLs.

Examples of DL2 functions include:

- Anticipatory plant trips
- Maintaining target power
- Maintaining target water level
- Maintaining target pressure
- Control rod blocks

3.3 Defense Line 3

The third line of defense is established for the very unlikely event (1E-02 to 1E-05 per reactor-year frequency) where certain AOOs escalate into DBA Fault Sequences through failures beyond the AOO PIEs, and for PIEs that by frequency result in DBA Fault Sequences.

DBAs are evaluated in the Safety Analysis, crediting the DL3 functions that act to mitigate DBA Fault Sequences by preventing fuel damage, assuring the integrity of the barriers preventing fission product release, and placing and maintaining the plant in a safe state until normal operations are resumed.

PIEs or Fault Sequences in the DBA frequency range include but are not limited to:

- Single failure of non-SC1 passive equipment
- Single failure of SC1 digital equipment
- Single failure of SC1 passive equipment
- Spurious CCF of non-SC1 digital equipment
- Spurious CCF of non-SC1 digital active equipment
- Internal and external hazard PIEs that are in the DBA frequency range of 1E-02 to 1E-05 per reactor-year

The SSCs involved in performance of DL3 functions are designed for high reliability, and are classified as SC1 meeting the definition of safety-related SSCs described in USNRC 10 CFR 50.2 and CNSC REGDOC-2.5.2, Section 7.1 "Safety classification of structures, systems and components." The DBA acceptance criteria comply with the regulatory requirements of USNRC 10 CFR 50.46 and CNSC REGDOC-2.4.1, Section 4.3.4. The DL3 functions and SSCs performing those functions are subject to functional and design requirements derived from the CN-DSA. Examples of DL3 functions include:

- Reactor Scram
- Isolation Condenser Initiation
- Main Steam Isolation
- Containment Isolation
- RPV Isolation

3.4 Defense Line 4

The purpose of the fourth line of defense is to mitigate DEC Fault Sequences that have a frequency less than 1E-05 per reactor-year, including those that are postulated to result in core damage.

DL4 is comprised of two subsets of DL functions that are designated as DL4a and DL4b and are performed by SC2 and SC3 SSCs, respectively. DL4a functions mitigate DEC Fault Sequences that occur without core damage. DL4b functions prevent or mitigate the consequences of SAs with postulated core damage.

DL4a functions are those that place and maintain the plant in a safe state for DEC Fault Sequences involving the following:

- DEC Fault Sequences involving escalation of DBA Fault Sequences resulting from assumed failure of DL3 function(s) with a frequency less than 1E-05 per reactor-year
- DEC Fault Sequences for PIEs with a frequency less than 1E-05 per reactor-year considered as credible events, and which may involve multiple failures causing the loss of a FSF to be fulfilled as part of normal operation

Examples of DL4a functions include:

- Diverse means of achieving the FSFs that are independent of and diverse from the SSC carrying out the DL3 functions that are presumed to have failed
- Scrams initiated by the Diverse Protection System (DPS)

DL4b functions include the following:

- Functions provided in complex Fault Sequences that could lead to core damage, to either prevent core damage or limit the radiological releases in case of core damage, and are aimed at reasonably preserving the FSF of confinement of radioactive material (i.e., maintaining one or more fission product barriers functional) for extreme events, multiple events, or multiple failures that defeat DL2, DL3, and DL4a functions
- Functions provided to mitigate the effects from a damaged core and to reasonably preserve the FSF of confinement of radioactive material (i.e., maintaining one or more fission product barriers functional) while limiting radioactive releases to acceptable levels

Examples of DL4b functions include:

- DL4b measures carried out by complementary design features such as diverse and flexible equipment and portable components, such as portable uninterruptible power supplies and portable pumps
- RPV ultimate overpressure protection
- Containment venting and overpressure protection
- Boron injection

PIEs or Fault Sequences in the DEC frequency range generally include:

- Spurious CCF of SC1 digital or non-digital equipment
- Any AOO PIE plus mitigation of a CCF of SC1 equipment
- Any non-CCF DBA PIE plus mitigation of CCF of SC1 equipment

3.5 Defense Line 5

The fifth and final line of defense includes measures to cope with the radiological consequences of releases that could result from Severe Accidents which occur at a frequency of <1E-07 per reactor-year.

DL5 includes emergency preparedness measures to cope with potential unacceptable releases in case the first four DLs are not effective in maintaining the FSF of confinement of radioactive material (i.e., failure to maintain multiple fission product barriers functional). These are largely

measures taken to protect plant staff, emergency workers, and the public in a scenario involving substantial release of radiation.

Examples of DL5 measures include:

- SA management procedures
- Emergency response procedures and equipment (peripheral systems such as meteorological monitoring)
- Emergency response facility(ies), and certain communication systems (these measures may be initiated earlier in an event prior to progression to an SA)

3.6 Defense Line Independence

The BWRX-300 design incorporates independence in the application of D-in-D. DL functions that mitigate the same event are independent as far as is practicable to avoid the failure of one DL function reducing the effectiveness of other DL functions. Some examples include:

1. Among DL2, DL3 and DL4a functions, at least one DL function can mitigate a PIE caused by or concurrent with a CCF in another DL function, with the mitigation means being independent from the effects of the initiating CCF.
2. All PIEs with a frequency greater than 1E-05 per reactor-year caused by a single failure can be mitigated by DL3 functions and independently by DL2, DL4a, or a combination of DL2 and DL4a functions that are unaffected by the PIE. To the extent practicable, DL3 functions are independent and diverse from those in DL2 and from those in DL4a. This is because DL3 functions provide a backup to DL2 functions, and DL4a functions provide a backup to DL3 functions but DL4a functions are not needed to provide a direct backup to DL2 functions to maintain D-in-D for the same event.
3. The DL4b functions intended for mitigating DECs are functionally and physically separated from the systems intended for other DL functions.
4. DL4b SSCs specifically designed to mitigate the consequences of accidents with core damage are independent from SSCs used in normal operation or used to mitigate AOOs as far as is practicable and with exceptions justified.
5. Exceptions to rules of independence are described, assessed, and justified. If SSCs support functions in more than one DL, there is an increased focus on their reliability in the application of DL1 design process and quality measures as compared to a design feature credited in only one DL.

3.7 Classification of Structures, Systems and Components

The BWRX-300 approach to classifying SSCs meets the USNRC regulatory requirements and conforms to the guidance in USNRC SRP 19.3 and CNSC regulatory requirements and guidance in CNSC REGDOC-2.5.2. The classification approach incorporates selected guidance from IAEA SSR-2/1 and IAEA SSG-30.

Classification of SSCs is conducted to identify the importance of SSCs with respect to safety, consistent with the BWRX-300 Safety Strategy, and include the following areas:

- Safety Class (SC)
- Seismic Category
- Quality Classification

Classification of SSCs provides a means for applying appropriate design requirements and establishes a graded approach in the selection of materials, and application of codes and standards for civil, mechanical, I&C, and electrical SSCs used in design, manufacturing, construction, testing, and inspection of individual SSCs.

The BWRX-300 approach to classifying SSCs by SC is based primarily on deterministic methods and is directly traceable to the safety functions performed by each SSC. This approach meets the USNRC regulatory requirements and intent of the guidance in USNRC SRP 19.3 and CNSC regulatory requirements and guidance in CNSC REGDOC-2.5.2, Section 7.1, as it reflects the following:

- Consequences of the SSC failure to perform its safety functions
- Expected frequency of the SSC being called upon to perform its safety functions
- Time following a PIE at which, or the period for which, the SSC may be called upon to perform a safety function

A fundamental element of the BWRX-300 SSC classification approach is the direct correlation between the DL in which an SSC performs a function, and the relative safety importance of that function including risk significant functions. The safety classifications include:

- DL2 functions performed by SC3 SSCs
- DL3 functions performed by SC1 SSCs
- DL4a functions performed by SC2 SSCs
- DL4b functions performed by SC3 SSCs

4.0 BWRX-300 Safety Analysis

The BWRX-300 Safety Analysis complies with the following USNRC and CNSC regulatory requirements:

A. USNRC 10 CFR Part 20 “Standards for Protection Against Radiation”
    1) Subpart C- Occupational Dose Limits
        i. 10 CFR 20.1201 “Occupational dose limits for adults”
        ii. 10 CFR 20.1202 “Compliance with requirements for summation of external and internal doses”
        iii. 10 CFR 20.1203 “Determination of external dose from airborne radioactive material”
        iv. 10 CFR 20.1201 “Determination of internal dose exposure”
    2) Subpart D – Radiation Dose Limits for Individual Members of the public
        i. 10 CFR 20.1301 “Dose limits for individual members of the public”
        ii. 10 CFR 20.1302 “Compliance with dose limits for individual members of the public”

B. USNRC 10 CFR Part 50 “Domestic Licensing of Production and Utilization Facilities”

C. USNCR 10 CFR 50.34 “Contents of applications: technical information”
    1) 10 CFR 50.34(a)(1)(ii)(D) “Preliminary Safety Analysis report”

D. USNRC 10 CFR 50.46 “Acceptance criteria for emergency core cooling systems”

E. USNRC 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants”

F. USNRC 10 CFR Part 100 “Reactor Site Criteria”
    1) 10 CFR 100.11 “Determination of exclusion area, low population zone, and population center distance”

G. CNSC REGDOC-1.1.2 “Licence Application Guide: Licence to Construct Nuclear Power Plant”

H. CNSC REGDOC-2.4.1 “Deterministic Safety Analysis”

I. CNSC REGDOC-2.4.2 “Probabilistic Safety Assessment”

J. CNSC REGDOC-2.5.2 “Design of Reactor Facilities: Nuclear Power Plants”

The Safety Analysis includes:

- Hazards Analysis
- DSA
- PSA

The Safety Analysis primary objective is demonstrating that the FSFs are effective in:

- Controlling reactivity

- Removing heat from the fuel (reactor or fuel pool)
- Confining radioactive materials
  - Shielding against radiation
  - Controlling operational discharges
  - Limiting accidental releases

The BWRX-300 design basis is achieved through an iterative safety process. The design is implemented to meet defined safety objectives that are confirmed via the Safety Analysis. Results of the Safety Analysis provide feedback to the design. If indicated by the results, the design may be modified until safety objectives are met.

The BWRX-300 Safety Strategy framework integrates the DLs provided by implementing the D-in-D concept with the Safety Analysis. The D-in-D concept uses insights gained from operating experience and deterministic and RIPB analyses.

The RIPB graded quality assurance approach ensures that the USNRC SECY 94-084 and USNRC SECY 95-132 goals of specifying the reliability/availability (R/A) missions of risk-significant SSCs are met. Key elements of the RIPB process from SRP 19.3 include:

1. R/A missions of risk-significant SSCs related to performance, reliability, and availability of an SSC function adequately ensures the accomplishment of its task defined by the PRA and deterministic analysis.
2. R/A is implemented within the Safety Strategy process in establishing the missions for the risk-significant SSCs commensurate with the risk significance of those elements involved.
3. If active systems are determined to be risk-significant, the R/A missions are assessed as to whether the reliability availability program (RAP) and administrative controls on availability, or simple TS limiting conditions for operation (LCO) provide reasonable assurance that the missions are met during normal operation.
4. If equipment or systems are relied upon to meet the R/A mission, a graded quality assurance (QA) is applied commensurate with the risk significance.
5. The design process includes safety and non-safety deterministic requirements for R/A missions for risk-significant SSCs

The comprehensive baseline Probabilistic Risk Assessment (PRA) and PRA sensitivity studies are performed using a graded QA approach that ensures that SSCs relied upon under power operations and shutdown conditions meet the goals. The RIPB graded QA approach assures that non-safety class SSCs provide back-up to DL3 functions up to 72 hours after a DBA using DL2 and DL4a functions and provide reasonable assurance that those DL2 and DL4a SSCs can perform their necessary functions for a period up to 7 days following DBA.

The Safety Analysis is performed to demonstrate the effectiveness of the SSCs necessary to perform the functions assigned in various DLs that are credited to mitigate the PIEs. Figure 4-1 depicts the Safety Strategy implementation process into the Safety Analysis:

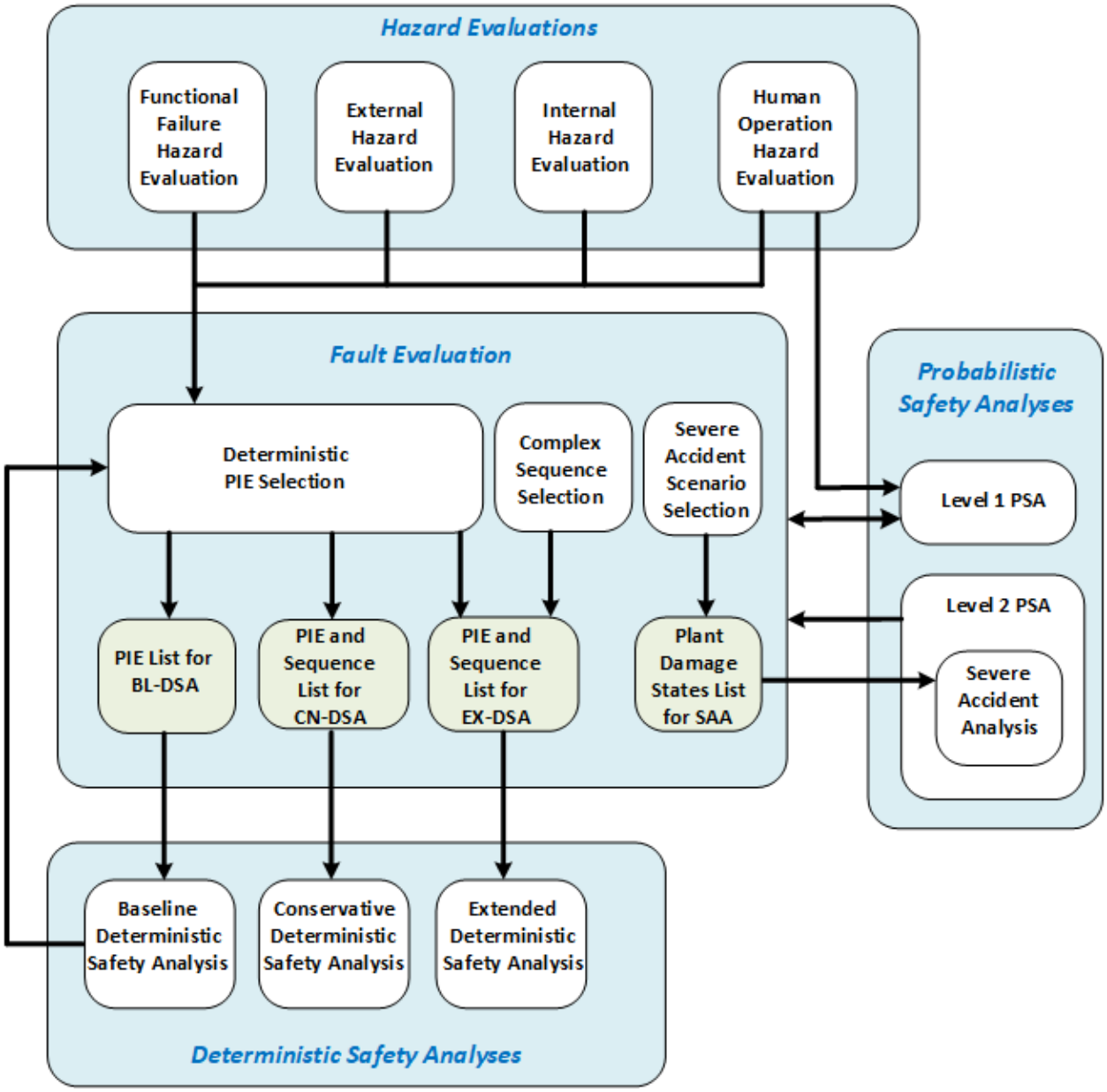

Figure 4-1: BWRX-300 Safety Strategy Implementation Process

4.1 Safety Analysis Objectives, Scope and Approach

The general nuclear safety objectives are demonstrated by the results from the Safety Analysis. As shown on Figure 4-1, there are of four types of Hazard Evaluations. The main objectives of the Hazard Evaluations are the identification of potential PIEs and confirmation that the plant design effectively responds to credible internal and external hazards.

The Safety Analysis objectives include:

- Demonstrating the design meets the acceptance criteria established following a graded approach for each plant state. The graded approach application may lead to acceptance criteria more restrictive for events with higher occurrence probability.

- Deriving and confirming TS or OLCs for normal operation
- Establishing and validating accident management procedures and guidelines

The Safety Analysis scope includes all plant states (see Figure 3-1) and include:

- Normal operation
- AOOs
- DBAs
- DECs may occur without or with core damage.

The BWRX-300 DSA uses a layered analysis approach that includes three types of DSA evaluations:

- Baseline – DSA (BL-DSA)
- Conservative – DSA (CN-DSA)
- Extended – DSA (EX-DSA)

This approach addresses initiating and mitigating DL function failures in a more systematic and structured manner than past approaches. The PSA is performed to complement the DSA. The PSA estimates the overall risk presented by the facility that is compared to the regulatory safety goals.

4.2 Analysis of Hazards

An initial step in performing the Safety Analysis is a systematic hazards evaluation. The BWRX-300 Safety Strategy process identifies four types of Hazard Evaluations for the complete range of plant states (full power, low power, load following, shutdown and refueling, and all fault sequences) that produces a comprehensive set of PIEs:

- Functional Failure Hazard Evaluation (FFHE)
- External Hazard Evaluation (EHE)
- Internal Hazard Evaluation (IHE)
- Human Operation Hazard Evaluation (HOHE)

The Hazard Evaluations include any consequential failure that occurs because of the PIE. They also address all sources of radioactivity (e.g., spent fuel, fuel being handled) in addition to the reactor core itself.

Each Hazard Evaluation identifies any potential challenges to an FSF.

4.2.1 Functional Failure Hazard Evaluation

The FFHE identifies failures of plant systems or equipment with potential to cause a challenge to an FSF. These hazards are identified in Failure Modes and Effect Analyses (FMEAs) performed on the plant systems.

The FFHE is limited to random single failures and to CCFs. The system FMEAs are reviewed to identify failures that cause challenges to FSFs. A consolidated list of failures from all system FMEAs is generated and organized.

The FFHE potential PIE sources are organized by quantitative frequency, using the frequency ranges defined in the Safety Strategy, and screened as potential PIEs evaluated in the Fault Evaluation and resulting DSA and PSA.

4.2.2 External Hazard Evaluation

The EHE includes site-specific natural and human-induced hazards that originate from a source that is not under control of the nuclear power plant license holder. The EHE addresses individual hazard sources and combinations of sources including:

- Natural external hazards including earthquakes, droughts, floods, high winds, tornadoes, tsunami, and extreme meteorological conditions
- Human-induced external hazards including toxic gas releases, aircraft crashes, or ship collisions

Once the site-specific external hazards are identified, the BWRX-300 structures are designed to provide protection from these external hazards for systems and equipment that perform FSFs inside the protected area of the site. Human-induced external hazards such as toxic gas and aircraft impacts are also evaluated in the design for control room habitability.

The sources of external hazard or combinations thereof are organized by quantitative frequency as potential PIEs evaluated in the Fault Evaluation. Malevolent acts are addressed in a separate security-related Hazard Evaluation.

4.2.3 Internal Hazard Evaluation

The IHE identifies hazards originating within the owner-controlled area of the site and with the potential to lead to an unplanned plant transient and damage to systems and equipment inside the protected area of the site. The internal hazard conditions do not directly challenge an FSF, but the effects of the hazard may cause system and equipment failures.

Internal hazards include:

- Fires
- Explosions and missiles from rotating or pressurized equipment
- Collapse of structures/falling objects
- Pipe whip, jet impingement, and flooding

The IHE addresses both individual hazard sources and combinations of sources.

The sources of internal hazard or combinations are organized by quantitative frequency as potential PIEs and evaluated in the Fault Evaluation and resulting DSA and PSA.

4.2.4 Human Operation Hazard Evaluation

The HOHE identifies erroneous decisions or human action(s) that lead to an unplanned plant transient. Human operations hazards typically involve unplanned changes to plant system and equipment status by equipment operators or maintenance personnel.

Many human operations hazards produce the same effects as corresponding system and equipment failures and the effects of these are included in the FFHE. The HOHE is limited to a single erroneous act that may lead to multiple system and equipment responses. The HOHE focuses on identifying unique hazards such as an operator initiating a group command on multiple actuators that is beyond what is considered in a single failure analysis of a particular system.

The sources of HOHE or combinations are organized by quantitative frequency as potential PIEs and evaluated in the Fault Evaluation and resulting DSA and PSA.

4.2.5 Analysis of Design Basis Conditions

The BWRX-300 design basis conditions are Normal Operations, AOOs and DBAs described below:

1. Normal Operation is operation within specified TSs and OLCs and includes the full range of plant operating modes. The objective of the Normal Operation Safety Analysis is to demonstrate that DL1 measures are effective in preventing abnormal operations and failures, thus meeting radiological requirements.
2. AOOs are deviations from normal operation that are expected to occur at least once during the operating lifetime of the reactor facility. The objective of the AOO Safety Analysis is to demonstrate that DL2 functions are effective for most AOO PIEs in meeting the applicable acceptance criteria.
3. DBAs conditions are identified as deviations from normal operations that are less frequent and more severe than AOOs. An objective of DBA Safety Analysis is to demonstrate that DL3 functions are effective in mitigating events and meeting the applicable acceptance criteria.

The response to AOOs and DBAs is achieved by SSCs specifically designed to mitigate these events and are assigned DL2 and DL3 functions.

4.2.6 Analysis of Design Extension Conditions Without Core Damage

DECs are postulated accident conditions that are less frequent than DBAs. DECs may occur with or without core damage.

DSA is performed for DECs without core damage demonstrating that releases of radioactive material are kept within acceptable limits and support the PSA determination of no core damage.

DEC analysis include:

- Multiple failures defined as complex sequences identified in the Level 1 PSA or as a PIE with a CCF

- AOO and DBAs with postulated failures of DL2 and DL3 functions analyzed in EX-DSA. For these events, the DBA acceptance criteria are used as screening criteria to the evaluation of core damage
- Low frequency events
- Non-reactor Fault Sequences (fuel pool accidents) are analyzed in Level 1 PSA

The analysis of DECs with core damage are addressed in the Level 2 PSA.

4.2.7 Analysis of Design Extension Conditions with Core Damage (Severe Accidents)

Severe Accidents (SAs) involve a catastrophic failure, core damage, and fission product release. An SA is generally considered to begin with the onset of core damage. To the extent that core damage is not practically eliminated, representative DECs with core damage are postulated to provide inputs for the containment design and safety features ensuring containment functionality. This set of accidents is considered in the design of corresponding safety features for DECs and represents a set of bounding cases.

SA sequences are selected that identify representative core damage scenarios and corresponding plant damage states that are used as the basis for performing the SA Analysis (SAA). The scope of SA scenario selection corresponds to sequences involving significant core damage that could lead to a containment breach and radioactive release analyzed in the Level 2 PSA. The selected SA scenarios are included in a Fault Evaluation.

The SAA goal is to provide input to accident management for terminating the progression of core damage, maintaining containment integrity as long as possible, and minimizing on-site and offsite radioactive material releases. Halting core damage progress could prevent Reactor Pressure Vessel (RPV) failure.

The response to SAs considers the use of permanent and temporary systems and equipment that function beyond their originally intended functions.

Using the guidance in IAEA SSR 2/1, Paragraph 2.11, Fault Sequences that could result in high radiation doses or in a large radioactive release are practically eliminated, and Fault Sequences with significant frequency of occurrence are shown to have no, or only minor, potential radiological consequences. Fault Sequences that are either physically impossible or extremely unlikely (<1E-09 per reactor-year) to occur are considered for Practical Elimination.

The Practical Elimination demonstration considers accumulated knowledge of BWRX-300 accident conditions and phenomena substantiated by relevant evidence.

4.3 Identification, Categorization and Grouping of PIEs and Accident Scenarios

A fundamental element of the Safety Analysis is the identification and selection of PIEs achieved through a systematic process of Fault Evaluation. The Fault Evaluation objective includes:

- Identification, categorization and grouping of PIEs or Fault Sequences
- Identification of the plant functions expected to be credited in the Safety Analysis and their assignment to a DL (DL2, DL3 and DL4)

The Fault Evaluation scope is the list of potential PIEs generated by the Hazards Evaluation and includes:

- Complete range of operating modes
- All radioactivity sources (nuclear fuel in the reactor core and nuclear fuel outside the reactor core)
- Single failure PIEs, CCF PIEs, and Fault Sequences developed based on the success or failure of mitigating functions. Single and CCF PIEs include system and equipment failures and human errors. CCF are analyzed as software platform or mechanical failures

The output of the Fault Evaluation establishes traceability between the plant design and the Safety Analysis. The Fault Evaluations start in parallel with or prior to DSA and PSA activities. DSA and PSA mature with the design and the Fault Evaluation is updated accordingly.

The Fault Evaluation includes the following activities as shown on Figure 4-1:

- Deterministic PIE Selection
- Complex Sequence Selection
- SA Scenario Selection

Deterministic PIE Selection

The deterministic PIE selection is the systematic process in organizing and selecting events for DSA. Selected PIEs and Fault Sequences are allocated to three DSA types in a fault list:

- PIE List for Baseline DSA (BL-DSA)
- PIE/Fault Sequence List for Conservative DSA (CN-DSA)
- PIE/Fault Sequence List for Extended DSA (EX-DSA)

Complex Sequence Selection

Complex sequences are Fault Sequences involving failures of multiple mitigating features, which have not been included in the deterministic PIE selection but are identified in the Level 1 PSA as having the potential to lead to core damage with a frequency of occurrence or consequences judged to require analysis and DL mitigation function. These complex sequences are added to the Fault Evaluation and analyzed in the EX-DSA.

SA Scenario Selection

The scope of SA sequence selection corresponds to those sequences involving significant core damage, which could lead to a breach of containment and radioactive release in the Level 2 PSA. To the extent that core damage is not practically eliminated, representative SA Fault Sequences (DECs with core damage) are postulated and analyzed in the SAA. The primary objective of the SA sequence selection is to identify representative core damage scenarios and define corresponding plant damage states that are used as the basis for performing the SAA. The selected SA scenarios are documented in the Fault Evaluation and analyzed in the SAA.

4.3.1 Basis for Categorization of PIEs, Accident Scenarios and Fault Evaluation

The Hazard Evaluations results in the list of potential PIEs. These potential PIEs are evaluated, categorized, and grouped during the Fault Evaluation in the deterministic PIE selection. The Hazard Evaluations address a complete range of plant modes of operation, all sources of radioactivity and any consequential failure that occurs because of the PIE. During design development, the Hazard Evaluation is validated, and PIE selection is updated accordingly.

The activities included in the deterministic PIE selection and their bases are presented below:

1. Fault Sequences development – a Fault Sequence is developed starting with a PIE and considers the success or failure of the required mitigating functions. The DL of each credited mitigating function is established for each Fault Sequence.
2. Fault Sequences are grouped into Fault Groups based on similar impact on a certain plant parameter: for example, events that lead to pressure increase in the reactor such as inadvertent closure of the Turbine Stop Valves and/or Turbine Control Valves or inadvertent closure of the Main Steam Reactor Isolation Valve(s) (MSRIVs) are grouped in the pressure increase Fault Group.
3. Fault Sequences are categorized within each fault group as AOO, DBA or DEC based on their frequency of occurrence.
4. Plant conditions are defined corresponding to each PIE supporting the scenario analysis.
5. Any exceptions are applied or justified to the standard PIE selection.

A bounding set of PIEs and Fault Sequences that result in the most significant challenge to the FSFs are selected for evaluation in the DSA. DSA layers and events categories are combined so that limiting baseline events are AOO (BL-AOO), the limiting CN events are DBAs (CN-DBA) and limiting EX events are DECs (EX-DEC). This notation is used to identify the layer and event category.

4.3.1.1 Baseline Deterministic Safety Analysis

The primary objective of the BL-DSA is demonstrating the effectiveness of the DL2 functions. The scope of BL-DSA includes single failure PIEs categorized as bounding BL-AOOs and BL-DBAs. The BL-DSA models are the expected response of the plant (no failure is postulated) to demonstrate that the event meets applicable acceptance criteria. The analysis end point is the controlled state condition. The mitigating DL functions credited in BL-DSA are DL2 functions. If a DL2 function fails or is not effective, then the corresponding DL3 function is credited.

4.3.1.2 Conservative Deterministic Safety Analysis

CN-DSA primary objective is demonstrating the effectiveness of DL3 functions. The CN-DSA scope includes events categorized as bounding CN-DBAs:

- PIEs due to single failure
- PIEs due to spurious CCF in DL2 or DL4a
- Baseline PIEs with postulated passive CCF of DL2 functions that were credited in BL-DSA

The CN-DSA is performed using conservative initial conditions with established acceptance criteria and applying a graded approach in quantifying the uncertainties. Single failure criterion is applied to DL3 SC1 components. CN-DSA credits only DL3 mitigation functions. The end point of the analysis is a controlled state condition.

4.3.1.3 Extended Deterministic Safety Analysis

The EX-DSA primary objective is assessing the effectiveness of DL4 functions. The EX-DSA scope includes events categorized as DECs:

- PIEs due to spurious CCF of DL3 functions
- DBA Fault Sequences with postulated passive CCF of DL3 mitigating functions
- Complex sequences identified by the Level 1 PSA

An extended sequence for AOOs and DBAs is required in the following conditions:

1. If a DL3 function is credited to mitigate a single failure PIE in the BL-DSA, then the DEC Fault Sequence assumes a passive CCF in DL3 functions (no additional mitigation single failure is assumed).
2. If the hydraulic scram action is credited in an BL-AOO scenario, then the hydraulic scram action is assumed to have a mechanical CCF of the hydraulic scram where only the Fine Motion Control Rod Drive (FMCRD) motor run-in functions insert control rods. No additional failures are assumed.

4.3.2 Categorization Events According to Their Frequencies

One fundamental element of the deterministic PIE selection and Fault Sequence selection is the assignment of Fault Sequences to categories based on their frequency of occurrence:

- AOO (frequency greater than 1E-02 per reactor-year)
- DBA (frequency between 1E-02 and 1E-05 per reactor-year)
- DEC (frequency less than 1E-05 per reactor-year)

Qualitative frequencies are adopted as an interim measure and are used in the early design stages to progress the performance of DSAs prior to availability of more mature PSA information. Quantitative frequencies based on Level 1 PSA results are adopted as the final, governing measure of the Fault Sequence.

A Fault Sequence consists of a combination of a PIE and can include an assumed failure of a mitigating function(s). The event category is based on the sequence frequency not only the PIE frequency. The event category assigned to a Fault Sequence may be different than the event category assigned to the PIE that initiated the sequence because the Fault Sequence may include additional failures that make the sequence less likely to occur.

In addition to the event categorization frequency, the categorized events are allocated the following DSA types:

- Baseline AOO (BL-AOO)
- Conservative DBA (CN-DBA)

- Extended DEC (EX-DEC)

4.3.3 Grouping of Events According to Type

One of the steps in Fault Evaluation is grouping the events according to their type. The Fault Evaluation includes external events, internal events, human operational errors, functional failures evaluated in hazard analysis, Level 1 PSA complex sequences and Level 2 PSA SA sequences.

PIEs (faults) are grouped according to the resultant change in plant parameter and is similar to groupings described in USNRC NUREG-0800, SRP 15.0, Section I Areas of Review, Section 1.B "Categorization According to Type" and CNSC REGDOC-2.4.1, Section 4.2.3 "Classification of events":

- Temperature decrease events – decrease in core coolant temperature
- Pressure increase events – increase in reactor pressure
- Reactivity increase events – reactivity and power distribution anomalies
- Inventory increase events – increase in reactor coolant inventory
- Inventory reduction events – decrease in reactor coolant inventory
- Non-reactor fault events – these events are non-core related such as fuel handling accident
- Radiological faults having dose consequences

Once the Fault Groups are identified, then the anticipated core physics response associated with each group is then selected. Once each group is identified, then the bounding Fault Sequence from that group is selected.

4.3.4 PIEs and Accident Scenarios

PIEs and event frequency are first determined qualitatively based on system conceptual design, previous similar designs, and OPEX. PIEs are evaluated in the Fault Evaluation where they are further screened for inclusion.

The bounding event selection is performed for events that are initiated at full power conditions (Mode 1 operating condition) because they are expected to result in the most significant challenge to the fission product barriers.

Bounding events are selected in each Fault Group, for each event category (e.g., AOO, DBA, DEC without core damage) and for the applicable DSA layer (e.g., baseline, conservative and extended). The resulting events selected are analyzed in the DSA. DEC events with core damage are part of the PSA and SAA.

The bounding event selection is performed for two event categories:

- Transient or non-LOCA
- LOCA scenarios

Acceptance criteria are established for AOOs, DBAs, DECs with and without core damage consistent with USNRC 10 CFR 50, Appendix A, GDCs 10, 12, 17, 20, 25, 26, 33, 34, USNRC 10 CFR 50.46, CNSC REGDOC-2.4.1, Section 4.3 "Acceptance criteria," and CNSC REGDOC-

2.5.2, Section 4.2.1 based upon the frequency of occurrence of the Fault Sequence evaluated in the DSA or PSA.

Implementation of the safety objectives established ensures that the BWRX-300 facility when operated achieves the highest standard of reactor safety that can be reasonably achieved. Qualitative acceptance criteria are defined and met for each AOO and DBA to confirm the effectiveness of plant systems in maintaining the integrity of physical barriers against releases of radioactive material.

Derived qualitative and quantitative acceptance criteria are used to analyze AOOs or DBAs. Qualitative acceptance criteria are supported by experimental data, prescribed by regulatory requirements, or prescribed by applicable codes and standards. The results of the quantitative Safety Analysis confirm the derived acceptance criteria (i.e., the limiting event in an event group).

5.0 Summary

The Safety Strategy uses a defense-in-depth (D-in-D) safety concept providing a layered and iterative approach to plant safety while meeting USNRC and CNSC regulatory requirements and guidance. The BWRX-300 Safety Strategy framework considers both the safety-importance and risk-significance of each structure, system, and component (SSC) to determine the design requirements and appropriate safety and quality classification for each SSC and meets the regulatory requirements of USNRC 10CFR50 and CNSC REGDOC-2.4.1, REGDOC-2.4.2 and REGDOC-2.5.2.